REMARKS

[0001] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1-3, 8-10, 13-16, 18, 19, 22-29, 31, 32, and 34-43 are presently pending. Claims amended herein are 1-3, 8-10, 13-16, 28, 29, and 40. Claims cancelled herein are 6, 7, 17, 20, 21, 30, and 33.

Formal Request for an Interview

[0002] If the Examiner's reply to this communication is anything other than allowance of all pending claims and the only issues that remain are minor or formal matters, then I formally request an interview with the Examiner. I encourage the Examiner to call me—the undersigned representative for the Applicant—so that we can talk about this matter so as to resolve any outstanding issues quickly and efficiently over the phone. Please contact me to schedule a date and time for a telephone interview that is most convenient for both of us. While email works great for me, I welcome your call as well. My contact information may be found on the last page of this response.

Claim Amendments

[0003] Without conceding the propriety of the rejections herein and in the interest of expediting prosecution, Applicant amends claims herein. Applicant amends claims to highlight claimed features. Such amendments are made to expedite prosecution and should not be construed as further limiting the claimed invention in response to the cited references. Furthermore, support for the amendments may be found in the specification including the claims as originally filed. Hence, no new matter is introduced via the amendments.

Substantive Matters

Claim Rejections under § 101

[0004] Claims 1-3, 6-10 and 13-15 are rejected under 35 U.S.C. § 101. Applicant respectfully traverses these rejections. Furthermore, in light of the amendments presented herein, Applicant submits that these rejections are moot and respectfully requests that the rejections be withdrawn. If the Examiner maintains the rejection of these claims, then Applicant requests additional guidance as to what is necessary to overcome the rejection.

Claim Rejections under § 103

[0005] Claims 1-3, 6-10 and 13-43 are rejected under 35 U.S.C. § 103. In light of the amendments and discussion presented herein, Applicant submits that these rejections are moot. Accordingly, Applicant asks the Examiner to withdraw these rejections.

[0006] The Examiner's rejections are based upon the following references in combination:

- **Elgamal:** *Elgamal, et al.,* US Patent No. 6,397,330 (issued May 28, 2002);
- **Liu:** *Liu, et al.,* US Patent No. 7,051,067 (issued May 23, 2006); and
- **Fielder:** *Fielder, et al.,* US Patent No. 5,963,646 (issued October 5, 1999).

Overview of the Application

[0007] The Application describes a technology for determining and signaling if encryption uses weak keys or algorithms in order to avoid a "false security" by intercepting cryptographic API calls. For each such API the tool verifies the encryption parameters used and makes sure that the keys are secure enough.

Cited References

[0008] The Examiner cites Elgamal as the primary reference, Liu as the secondary reference, and Fielder as the tertiary reference in obviousness-based rejections.

[0009] Elgamal describes a method and apparatus for controlling the use of cryptography such that products utilizing these controls may be exported in accordance with United States export laws, and/or imported into other countries that place additional restrictions on the use of cryptography.

[0010] Liu describes an object oriented mechanism for dynamically constructing service implementations to enforce restrictions on services provided to an application.

[0011] Fielder describes a secure deterministic encryption key generator.

Obviousness Rejections

Lack of *Prima Facie* Case of Obviousness (MPEP § 2142)

[0012] Applicant disagrees with the Examiner's obviousness rejections. Arguments presented herein point to various aspects of the record to demonstrate that all of the criteria set forth for making a prima facie case have not been met.

[0013] The Examiner rejects claims 1-3, 6, 7, 10, 13-21, 23-33 and 35-43 under 35 U.S.C. § 103(a) as being unpatentable over Elgamal in view of Liu. Applicant respectfully traverses the rejection of these claims. Furthermore, in light of the amendments presented herein, Applicant respectfully submits that the rejections are moot and asks the Examiner to withdraw the rejection of these claims.

Independent Claim 1

[0014] Applicant submits that the combination of Elgamal and Liu does not teach or suggest at least the following features as recited in this claim (as amended, with emphasis added):

A computer implemented method comprising:

establishing, via the computer, at least one cryptography service parameter threshold comprising a minimum level of security;

establishing, via the computer, at least one maximum cryptography service parameter threshold;

wherein **establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes establishing a plurality of correctness categories**, wherein each at least one of said plurality of **correctness categories includes** at least one

cryptography algorithm identifier and said plurality of **correctness categories includes** at least one correctness category **selected from a group of correctness categories consisting of authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms**;

selectively **detecting**, via the computer, a **request from an application submitted via an application programming interface to an operating system** of the computer, the request comprising a **request for at least one cryptography service at the computer**; and

selectively performing, via the computer, at least one correctness detection action **responsive to detecting the request** based on the requested cryptography service and the at least one cryptography service parameter threshold, wherein:

the at least one correctness detection action selectively performed includes suggesting at least one alternative cryptography service;

the at least one alternative cryptography service comprises a cryptography service which meets the minimum level of security; and

the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold includes **determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold**, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold, wherein the size of the cryptographic key is identified by bit length.

[0015] Neither Elgamal nor Liu, alone or in combination teach or suggest all of the elements and features of this claim. Instead, the references teach a *conformance test* to determine that a particular algorithm having a configured key size is performing as expected based on known compliant implementations of the same algorithm. And, determining whether a client is authorized to access a resource via an API. For example, the Office relies on Liu as "disclos[ing] an

object oriented mechanism for dynamically constructing customized cryptographic service implementations on a per request bases, wherein the mechanism checks for a general implementation of a service, and if a general implementation is found, the mechanism then determines if the implementation is authentic. (6:5-31) see Action p. 7.

[0016] Notably, the claim does not require "*check[ing] for a general implementation of a service, and if a general implementation is found, the mechanism then determines if the implementation is authentic*" as taught by the reference because the operation of the claim occurs at request time—before implementation. As recited in the claim, "selectively **detecting**, via the computer, a **request from an application submitted via an application programming interface to an operating system** of the computer, the request comprising a **request for at least one cryptography service at the computer** ... ." Accordingly, and for at least this reason, Applicant asks the Examiner to withdraw the rejection of this claim.

Independent Claims 16 and 29

[0017] Independent claims 16 and 29 each include at least one feature similar to the claimed features as explained above with respect to claim 1. As indicated above with regard to claim 1, the combination of Elgamal and Liu does not teach or suggest these feature(s). Thus independent claims 16 and 29 are allowable over the cited references for at least similar reasons as claim 1. Accordingly, Applicant asks the Examiner to withdraw the rejection of these claims.

Dependent Claims 2, 3, 8-10, 13-15, 18, 19, 22-28, 31, 32, and 34-43

[0018] These claims ultimately depend upon one of independent claims 1, 16, and 29. As discussed above, claims 1, 16, and 29 are allowable over the cited documents. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable over the cited documents. Additionally, some or all of these claims may also be allowable for additional independent reasons.

[0019] Furthermore, the rejection of claims 8, 9, 22, and 34 are based on a combination of Elgamal in view of Liu and further in view of Fielder. However, Fielder does not remedy the deficiencies of Elgamal and Liu as discussed above. Thus, Applicant respectfully traverses the rejection of these claims and asks the Examiner to withdraw the rejection of these claims.

Dependent Claims

[0020] In addition to its own merits, each dependent claim is asserted allowable for the same reasons that its base claim is allowable. Applicant requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

Conclusion

[0021] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action**. Please call or email me at your convenience.

Respectfully Submitted,

Lee & Hayes, PLLC
Representatives for Applicant

/Bea Koempel-Thomas 58213/ Dated: 05/11/09
Beatrice L. Koempel-Thomas (bea@leehayes.com; 509-944-4759)
Registration No. 58213

Assistant: Cherri Simon (cherri@leehayes.com; 509-944-4776)

Customer No. **22801**

Telephone: (509) 324-9256
Facsimile: (509) 323-8979
www.leehayes.com